

TELEFAX COVER SHEET

PATTERSON & SHERIDAN, LLP
ATTORNEYS AT LAW
595 SHREWSBURY AVENUE
FIRST FLOOR
SHREWSBURY, NJ 07702
TELEPHONE (732) 530-9404
TELEFAX (732) 530-9808

RECEIVED
CENTRAL FAX CENTER

APR 17 2006

THIS TELEFAX MESSAGE IS ADDRESSED TO THE PERSON OR COMPANY LISTED BELOW.
IF IT WAS SENT OR RECEIVED INCORRECTLY, OR YOU ARE NOT THE INTENDED
RECIPIENT, PLEASE TAKE NOTICE THAT THIS MESSAGE MAY CONTAIN PRIVILEGED OR
CONFIDENTIAL MATERIAL, AND YOUR DUE REGARD FOR THIS INFORMATION IS
NECESSARY. YOU MAY ARRANGE TO RETURN THIS MATERIAL BY CALLING THE FIRM
LISTED ABOVE AT (732) 530-9404

THIS MESSAGE HAS 34 PAGES INCLUDING THIS SHEET

TO: Commissioner of Patents
FAX NO.: 571-273-8300
FROM: Kin-Wah Tong, Esq.
DATE: April 17, 2006
MATTER: Serial No 09/682,526 Filed: September 14, 2001
DOCKET NO.: ATT 2000-0415
APPLICANT: RUBIN

The following has been received in the U.S. Patent and Trademark Office on the date of this facsimile:

<input type="checkbox"/> Petition	<input checked="" type="checkbox"/> Transmittal Form
<input type="checkbox"/> Disclosure Statement & PTO-1449	<input checked="" type="checkbox"/> Fee Transmittal (2 copies)
<input type="checkbox"/> Priority Document	<input checked="" type="checkbox"/> Deposit Account Transaction
<input type="checkbox"/> Revocation and Appointment of Attorney	<input checked="" type="checkbox"/> Facsimile Transmission Certificate dated <u>April 17, 2006</u>
<input type="checkbox"/> Extension Request (one month)	
<input checked="" type="checkbox"/> Appeal Brief	

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8

I hereby certify that this correspondence is being transmitted by facsimile to the Commissioner for Patents,
P.O. Box 1450, Alexandria, VA 22313 on April 17, 2006, Facsimile No. 571-273-8300.

Kin-Wah Tong
Name of person signing this certificate


Signature and date April 17, 2006

**RECEIVED
CENTRAL FAX CENTER**

Please type a plus sign (+) inside this box → ☒**APR 17 2006**

PTO/SB/21 (08-03)

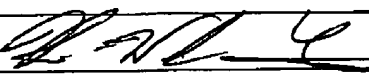
Approved for use through 7/31/2008. OMB 0651-0031


U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)		Application Number	09/682,526
		Filing Date	September 14, 2001
		First Named Inventor	RUBIN
		Group Art Unit	2131
		Examiner Name	Arezoo Sherkat
Total Number of Pages in This Submission		Attorney Docket Number	ATT/2000-0415

ENCLOSURES (check all that apply)						
<input type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment / Response <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request (1 month) <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/ Incomplete Application <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____	<input type="checkbox"/> After Allowance Communication to Group <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): <p align="center">Certificate of Facsimile Transmission</p>				
<table border="1"> <tr> <td align="center" colspan="2">Remarks</td> </tr> <tr> <td colspan="2" style="height: 40px;"></td> </tr> </table>			Remarks			
Remarks						

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	Kin-Wah Tong, Reg. No. 39,400 PATTERSON & SHERIDAN
Signature	
Date	April 17, 2006

CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.			
Typed or printed name	KIN-WAH TONG	Date	April 17, 2006
Signature			

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon on the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

RECEIVED
CENTRAL FAX CENTER

APR 17 2006

PTO/SB/17 (12-04v2)

Approved for use through 07/31/2006. OMB 0851-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL for FY 2005

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$)

\$500.00

Complete if Known

Application Number 09/882,526
Filing Date September 14, 2001
First Named Inventor RUBIN
Examiner Name Arezoo Sherkat
Art Unit 2131
Attorney Docket No. ATT/2000-0415

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☒ None ☐ Other (please identify) :

☒ Deposit Account Deposit Account Number 20-0782 Deposit Account Name: Patterson & Sheridan LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayments of fee(s) ☒ Credit any overpayments

Under 37 CFR 1.16 and 1.17

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description

Each claim over 20 (including Reissues)
Each independent claim over 3 (including Reissues)
Multiple dependent claims

Small Entity Fee (\$)	Fee (\$)
50	25
200	100
360	180

Total Claims Extra Claims Fee (\$) Fee Paid (\$)

-20 or HP= x =

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims Extra Claims Fee (\$) Fee Paid (\$)

- 3 or HP= x =

HP = highest number of independent claims paid for, if greater than 3.

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets Extra Sheets Number of each additional 50 or fraction thereof Fee (\$) Fee Paid (\$)

- 100 = / 50 = (round up to a whole number) x =

4. OTHER FEE(S)


Non-English Specification, \$130 fee (no small entity discount)

Other (e.g., late filing surcharge): Appeal Brief

Fees Paid (\$)

500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	39,400	Telephone	(732) 530-8404
Name (Print/Type)	Kin-Wah Tong	Date	April 17 2006		

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing this form, call 1-800-PTO-8198 (1-800-786-9199) and select option 2.

RECEIVED
CENTRAL FAX CENTER

APR 17 2006

PATENT
Atty. Dkt. No. 2000-0415

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

**In re Application of:
Aviel D. Rubin**

Serial No.: 09/682,526

Confirmation No.: 3764


Filed: September 14, 2001

For: **METHOD FOR SECURE
REMOTE BACKUP**

Group Art Unit: 2131

Examiner: Arezoo Sherkat

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or being facsimile transmitted to the USPTO, on the date indicated below.	
April 17, 2006	
Date	Signature

Dear Sir:

APPEAL BRIEF

Appellant submits this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2131 dated October 19, 2005, finally rejecting claims 1-16. Please charge the fee of \$500.00 for filing this brief and all other fees that may be required to make this Brief timely and acceptable to the Patent Office, to Deposit Account No. 20-0782/ATT2000-0415.

REAL PARTY IN INTEREST

The real party in interest is AT&T, Corp.

04/19/2006 BABRAHA1 00000029 200782 09682526
01 FC:1402 500.00 DA

BRIEF ON APPEAL
Serial No. 09/682,526
Page 2 of 30

RELATED APPEALS AND INTERFERENCES

The Appellant knows of no related appeals or interferences that might directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-16 are pending in the application. Claims 1-16 were originally presented in the application. Claims 1-16 stand rejected in view of several references as discussed below. The rejection of claims 1-16 based on the cited references is appealed. The pending claims are shown in the attached Appendix.

STATUS OF AMENDMENTS

Claims 5 and 13 were amended in a response to an Office Action dated August 2, 2004, filed on December 2, 2004, to correct informalities. No amendments to the claims, in this application, were submitted subsequent to final rejection. The Appellant is appealing the claims as they read at the time the final rejection was issued. These claims are shown in the attached Appendix.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides for a method and device-readable medium storing program instructions pertaining to backing up one or more files on a local device onto remote servers over a network. In the embodiment of independent claim 1, the invention comprises deriving (303) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, pg. 4, para. [0014].) Then the method compresses (304) one or more files and adds (304) each of the files to a bundle (200). (See *Id.* at pg. 5, para. [0015].) Next, an authentication code (228) for the bundle (200) using the first cryptographic key is generated (306) and the authentication code (228) is added to the bundle (306). (See *Id.*) The method concludes by encrypting (307) the bundle (200) using the second cryptographic key prior to sending the bundle to the remote server. (See *Id.*)

In the embodiment of independent claim 5, a method for restoring one or more files

BRIEF ON APPEAL
Serial No. 09/682,526
Page 3 of 30

on remote servers to a local device over a network is described. The method comprises deriving (402) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, page 6, para. [0019].) Then the method decrypts (407) a bundle (200) received from the remote server using the second cryptographic key. (See *Id.*) Next, an authentication code (228) in the bundle (200) is checked (408) using the first cryptographic key. (See *Id.*) The method concludes by decompressing (409) one or more files from the bundle (200). (See *Id.*)

In the embodiment of independent claim 9, a device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network is described. The program instructions for the method stored on the device-readable medium comprises deriving (303) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, pg. 4, para. [0014].) Then the method compresses (304) one or more files and adds (304) each of the files to a bundle (200). (See *Id.* at pg. 5, para. [0015].) Next, an authentication code (228) for the bundle (200) using the first cryptographic key is generated (306) and the authentication code (228) is added to the bundle (306). (See *Id.*) The method concludes by encrypting (307) the bundle (200) using the second cryptographic key prior to sending the bundle to the remote server. (See *Id.*)

In the embodiment of independent claim 13, a device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network is described. The program instructions for the method stored on the device-readable medium comprises deriving (402) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, page 6, para. [0019].) Then the method decrypts (407) a bundle (200) received from the remote server using the second cryptographic key. (See *Id.*) Next, an authentication code (228) in the bundle (200) is checked (408) using the first cryptographic key. (See *Id.*) The method concludes by decompressing (409) one or more files from the bundle (200). (See *Id.*)

BRIEF ON APPEAL
Serial No. 09/682,526
Page 4 of 30

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-2, 4-6, 8-10, 12-14 and 16 stand rejected under 35 U.S.C. §103(a) as being obvious over Bailey, III (U.S. Patent 5,659,614, issued August 19, 1997, hereinafter referred to as "Bailey") in view of Cane, et al. (U.S. Patent 5,940,507, issued August 17, 1999, hereinafter referred to as "Cane"). Claims 3, 7, 11 and 15 stand rejected under 35 U.S.C. §103(a) as being obvious over Bailey in view Cane in further view of Walmsley (US Publication 2004/0049468, published March 11, 2004, hereinafter referred to as "Walmsley").

ARGUMENT

A. 35 U.S.C. §103(a) – Bailey in view of Cane

1. Claim 1

The Examiner has rejected claim 1 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

Bailey teaches a method and system for creating and storing a backup copy of file data stored on a computer. "The file data to be backed up is encrypted using multiple, indirect encryption keys, variable block lengths, and variable algorithms based on a client-selected string of characters. The files are thereafter encrypted again at the client site prior to transmission to the backup site. A program registry is maintained at the backup site that contains a master copy of many commercially-available files. The incoming files received from the client site are compared to the files in the program registry. If an incoming file is located in the registry, the file is replaced by a token identifying the commercially-available file and the token is stored at the backup facility." (See Bailey, Abstract.)

Cane teaches an information process system that provides archive/backup support with privacy assurance by encrypting relevant stored data. Notably, data generated on a source system is encrypted, the key used thereby is separately encrypted, and both the encrypted data and encrypted key are transmitted to and maintained by a data repository system. (See Cane, Abstract.)

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination, fails to teach or to suggest the novel concept

BRIEF ON APPEAL
Serial No. 09/682,526
Page 5 of 30

of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle, as positively claimed by the Appellant's independent claim 1. Specifically, Appellant's independent claim 1 positively recites:

1. A method of backing up one or more files on a local device onto remote servers over a network comprising:
deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
compressing one or more files and adding each of the files to a bundle;
generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added.)

In one embodiment, the Appellant's invention provides a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and authentication properties make them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the

BRIEF ON APPEAL
Serial No. 09/682,526
Page 6 of 30

transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key," emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5).

Cane fails to bridge the substantial gap left by Bailey because Cane specifically teaches using a cryptographic engine 14 and key generator 16. (See Cane, col. 3, ll. 51 and 56, FIG. 1.) Similar to the gap found in Bailey, Cane's keys are also not derived from a user-provided passphrase. As such, this element in Appellant's claims is completely absent in both references.

Moreover, as indicated by the Examiner on page 3 of the Final Office Action, Bailey fails to disclose the generation of an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle. However, the Examiner alleges that Cane teaches this limitation. The Examiner specifically points to Cane, col. 4, ll. 1-27.

The Appellant respectfully submits that the Examiner has interpreted Cane too broadly and must look at Cane in its entirety. The passage cited by the Examiner reads:

"Transmission may be accomplished via Internet 26, dialup connection 28, or in alternative embodiments, other means such as physical delivery of the storage medium. Encryption may be performed by any of various known methods, such as RSA, DES, and other permutations and may involve authentication and verification either through a trusted third party or mathematical methods. Such authentication and verification may involve cipher block chaining (CBC), to perform an XOR on all or part of a previous block and use the resultant value in encrypting a successive block, or checksums such as cyclic redundancy checks (CRC), MD4, and MD5, which accumulate all values in a particular block according to a mathematical formula to arrive at a value which is highly unlikely to be duplicated if data in the block is changed or lost."

BRIEF ON APPEAL
Serial No. 09/682,526
Page 7 of 30

The Appellant respectfully submits that this passage clearly fails to specifically teach generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle, as positively recited in the Appellant's independent claim 1. The portion of the cited passage mentioning "transmissions" refers to the transmission of encrypted file 20 and encrypted key 24 mentioned earlier in the paragraph and not to the following discussion on encryption. Therefore, contrary to the Examiner's assertion, this passage does not teach that checksums such as CRC, MD4 and MD5 are a part of the "transmission". The Appellant respectfully submits that the cited passage in Cane at best generally describes the various methods of encryption and authentication and not generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle, as positively claimed by the Appellant's independent claim 1.

Furthermore, the alleged combination (as taught by Cane) clearly teaches away from the Appellant's invention because Cane teaches that a master key is obtained and used to encrypt a secondary key and produce an encrypted key that is separate from the encrypted file. (See Cane, col. 3, ll. 56-61, emphasis added.) The encrypted file and the encrypted key are then transmitted as separate entities (i.e. not in a single bundle or file) to the archive server as indicated in separate steps 116 and 118. (See Cane, FIG. 2.) Consequently, the Appellant respectfully submits that independent claim 1 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

2. Claim 2

Claim 2 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 1. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 1, dependent claim 2 is also not made obvious since the claim depends directly from claim 1 and recites additional features of the present invention.

BRIEF ON APPEAL
Serial No. 09/682,526
Page 8 of 30

Thus, claim 2 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim 2. Encrypting the bundle with a strong block cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 2 is patentable under the provisions of 35 U.S.C. §103.

3. Claim 4

Claim 4 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 1. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 1, dependent claim 4 is also not made obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 4 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 4. Cryptographic keys containing at least 128 bits ensures greater security. This novel approach is absent in the alleged

BRIEF ON APPEAL
Serial No. 09/682,526
Page 9 of 30

combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 4 is patentable under the provisions of 35 U.S.C. §103.

4. Claim 5

The Examiner has rejected claim 5 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The teachings of Bailey and Cane are discussed above.

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination, fails to teach or to suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle, as positively claimed by the Appellant's independent claim 5. Specifically, Appellant's independent claim 5 positively recites:

5. A method of restoring one or more files on remote servers to a local device over a network comprising:
deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
decrypting a bundle received from the remote server using the second cryptographic key;
checking an authentication code in the bundle using the first cryptographic key; and
decompressing one or more files from the bundle. (Emphasis added.)

In one embodiment, the Appellant's invention provides a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and

BRIEF ON APPEAL
Serial No. 09/682,526
Page 10 of 30

authentication properties make them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key," emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5). Cane fails to bridge the substantial gap left by Bailey because Cane specifically teaches using a cryptographic engine 14 and key generator 16. (See Cane, col. 3, ll. 51 and 56, FIG. 1.) Similar to the gap found in Bailey, Cane's keys are also not derived from a user-provided passphrase. As such, this element in Appellant's claims is completely absent in both references.

Appellant also respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a method for restoring files on remote servers to a local device over a network comprising checking for an authentication code in the compressed bundle. As indicated on page 4 of the Final Office Action by the Examiner, Bailey does not expressly disclose the checking of an authentication code in the bundle using the first cryptographic key. However, the Examiner alleges that Cane teaches this limitation.

The Appellant respectfully submits that Bailey and Cane do not disclose, mention or suggest the checking of an authentication code in a bundle using the first cryptographic key. More specifically, the Appellant contends that Cane only teaches an

BRIEF ON APPEAL
Serial No. 09/682,526
Page 11 of 30

archive server that first writes the encrypted file to a medium and subsequently writes the encrypted key to another medium separately. Notably, the Appellant submits that Cane does not teach a checking process of any type. Therefore, the Appellant contends that since a bundle comprising an authentication code along with a plurality of files is not taught by Cane, it is impossible for the bundle to be checked (i.e., since a bundle does not exist.)

In fact, the alleged combination (as taught by Cane) teaches away from the Appellant's invention because the recovery process taught by Cane specifically teaches that first the secondary key must be recovered by decrypting the encrypted key with the master key, which is located separately on cryptographic engine 14. (See Cane, col. 4, ll. 27-37, FIG 1.) Then the original file is recovered by decrypting the encrypted file with the secondary key, which is also located separately. (See *Id.*) Consequently, the Appellant respectfully submits that independent claim 5 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

5. Claim 6

Claim 6 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 5. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 5, dependent claim 6 is also not made obvious since the claim depends directly from claim 5 and recites additional features of the present invention. Thus, claim 6 should be deemed patentable for at least the reasons stated above with respect to independent claim 5.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim 6. Encrypting the bundle with a strong block

BRIEF ON APPEAL
Serial No. 09/682,526
Page 12 of 30

cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 6 is patentable under the provisions of 35 U.S.C. §103.

6. Claim 8

Claim 8 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 5. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 5, dependent claim 8 is also not made obvious since the claim depends directly from claim 5 and recites additional features of the present invention. Thus, claim 8 should be deemed patentable for at least the reasons stated above with respect to independent claim 5.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 8. Cryptographic keys containing at least 128 bits ensures greater security. This novel approach is absent in the alleged combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 8 is patentable under the provisions of 35 U.S.C. §103.

7. Claim 9

The Examiner has rejected claim 9 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The teachings of Bailey and Cane are discussed above.

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination, fails to teach or to suggest the novel concept

BRIEF ON APPEAL
Serial No. 09/682,526
Page 13 of 30

of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle, as positively claimed by the Appellant's independent claim 9. Specifically, Appellant's independent claim 9 positively recites:

9. A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

compressing one or more files and adding each of the files to a bundle;

generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and

encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added.)

In one embodiment, the Appellant's invention provides a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and authentication properties make them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a

BRIEF ON APPEAL
Serial No. 09/682,526
Page 14 of 30

second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key.", emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5). Cane fails to bridge the substantial gap left by Bailey because Cane specifically teaches using a cryptographic engine 14 and key generator 16. (See Cane, col. 3, ll. 51 and 56, FIG. 1.) Similar to the gap found in Bailey, Cane's keys are also not derived from a user-provided passphrase. As such, this element in Appellant's claims is completely absent in both references.

Moreover, as indicated by the Examiner on page 3 of the Final Office Action, Bailey fails to disclose the generation of an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle. However, the Examiner alleges that Cane teaches this limitation. The Examiner specifically points to Cane, col. 4, ll. 1-27.

The Appellant respectfully submits that the Examiner has interpreted Cane too broadly and must look at Cane in its entirety. The passage cited by the Examiner reads:

"Transmission may be accomplished via Internet 26, dialup connection 28, or in alternative embodiments, other means such as physical delivery of the storage medium. Encryption may be performed by any of various known methods, such as RSA, DES, and other permutations and may involve authentication and verification either through a trusted third party or mathematical methods. Such authentication and verification may involve cipher block chaining (CBC), to perform an XOR on all or part of a previous block and use the resultant value in encrypting a successive block, or checksums such as cyclic redundancy checks (CRC), MD4, and MD5, which accumulate all values in a particular block according to a mathematical formula to arrive at a value which is highly unlikely to be duplicated if data in the block is changed or lost."

BRIEF ON APPEAL
Serial No. 09/682,526
Page 15 of 30

The Appellant respectfully submits that this passage clearly fails to specifically teach generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle, as positively recited in the Appellant's independent claim 9. The portion of the cited passage mentioning "transmissions" refers to the transmission of encrypted file 20 and encrypted key 24 mentioned earlier in the paragraph and not to the following discussion on encryption. Therefore, contrary to the Examiner's assertion, this passage does not teach that checksums such as CRC, MD4 and MD5 are a part of the "transmission". The Appellant respectfully submits that the cited passage in Cane at best generally describes the various methods of encryption and authentication and not generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle, as positively claimed by the Appellant's independent claim 9.

Furthermore, the alleged combination (as taught by Cane) clearly teaches away from the Appellant's invention because Cane teaches that a master key is obtained and used to encrypt a secondary key and produce an encrypted key that is separate from the encrypted file. (See Cane, col. 3, ll. 56-61, emphasis added.) The encrypted file and the encrypted key are then transmitted as separate entities (i.e. not in a single bundle or file) to the archive server as indicated in separate steps 116 and 118. (See Cane, FIG. 2.) Consequently, the Appellant respectfully submits that independent claim 9 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

8. Claim 10

Claim 10 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 9. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 9, dependent claim 10 is also not made obvious since the claim depends directly from claim 9 and recites additional features of the present invention.

BRIEF ON APPEAL
Serial No. 09/682,526
Page 16 of 30

Thus, claim 10 should be deemed patentable for at least the reasons stated above with respect to independent claim 9.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim 10. Encrypting the bundle with a strong block cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 10 is patentable under the provisions of 35 U.S.C. §103.

9. Claim 12

Claim 12 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 9. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 9, dependent claim 12 is also not made obvious since the claim depends directly from claim 9 and recites additional features of the present invention. Thus, claim 12 should be deemed patentable for at least the reasons stated above with respect to independent claim 9.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 12. Cryptographic keys containing at least 128 bits ensures greater security. This novel

BRIEF ON APPEAL
Serial No. 09/682,526
Page 17 of 30

approach is absent in the alleged combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 12 is patentable under the provisions of 35 U.S.C. §103.

10. Claim 13

The Examiner has rejected claim 13 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The teachings of Bailey and Cane are discussed above

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination, fails to teach or to suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle, as positively claimed by the Appellant's independent claim 13. Specifically, Appellant's independent claim 13 positively recites:

13. A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:
provided passphrase;

decrypting a bundle received from the remote server using the second cryptographic key;

checking an authentication code in the bundle using the first cryptographic key; and

decompressing one or more files from the bundle. (Emphasis added.)

In one embodiment, the Appellant's invention provides a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and authentication properties make

BRIEF ON APPEAL
Serial No. 09/682,526
Page 18 of 30

them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key," emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5). Cane fails to bridge the substantial gap left by Bailey because Cane specifically teaches using a cryptographic engine 14 and key generator 16. (See Cane, col. 3, ll. 51 and 56, FIG. 1.) Similar to the gap found in Bailey, Cane's keys are also not derived from a user-provided passphrase. As such, this element in Appellant's claims is completely absent in both references.

Appellant also respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising checking for an authentication code in the compressed bundle. As indicated on page 4 of the Final Office Action by the Examiner, Bailey does not expressly disclose the checking of an authentication code in the bundle using the first cryptographic key. However, the Examiner alleges that Cane teaches this limitation.

The Appellant respectfully submits that Bailey and Cane do not disclose, mention or suggest the checking of an authentication code in a bundle using the first cryptographic key. More specifically, the Appellant contends that Cane only teaches an

BRIEF ON APPEAL
Serial No. 09/682,526
Page 19 of 30

archive server that first writes the encrypted file to a medium and subsequently writes the encrypted key to another medium separately. Notably, the Appellant submits that Cane does not teach a checking process of any type. Therefore, the Appellant contends that since a bundle comprising an authentication code along with a plurality of files is not taught by Cane, it is impossible for the bundle to be checked (i.e., since a bundle does not exist.)

In fact, the alleged combination (as taught by Cane) teaches away from the Appellant's invention because the recovery process taught by Cane specifically teaches that first the secondary key must be recovered by decrypting the encrypted key with the master key, which is located separately on cryptographic engine 14. (See Cane, col. 4, ll. 27-37, FIG 1.) Then the original file is recovered by decrypting the encrypted file with the secondary key, which is also located separately. (See *Id.*) Consequently, the Appellant respectfully submits that independent claim 13 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

11. Claim 14

Claim 14 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 13. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 13, dependent claim 14 is also not made obvious since the claim depends directly from claim 13 and recites additional features of the present invention. Thus, claim 14 should be deemed patentable for at least the reasons stated above with respect to independent claim 13.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim

BRIEF ON APPEAL
Serial No. 09/682,526
Page 20 of 30

14. Encrypting the bundle with a strong block cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 14 is patentable under the provisions of 35 U.S.C. §103.

12. Claim 16

Claim 16 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Cane do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 13. Since Bailey and Cane do not make obvious the Appellant's invention as recited in Appellant's independent claim 13, dependent claim 16 is also not made obvious since the claim depends directly from claim 13 and recites additional features of the present invention. Thus, claim 16 should be deemed patentable for at least the reasons stated above with respect to independent claim 13.

Secondly, the Appellant contends that the combination of Bailey and Cane does not teach the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 16. Cryptographic keys containing at least 128 bits ensures greater security. This novel approach is absent in the alleged combination of Bailey with Cane. Thus, the Appellant respectfully submits that claim 16 is patentable under the provisions of 35 U.S.C. §103.

B. 35 U.S.C. §103(a) – Bailey and Cane in view of Walmsley

1. Claim 3

The Examiner has rejected claim 3 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Cane, and in further view of Walmsley. Appellants respectfully traverse the rejection.

BRIEF ON APPEAL
Serial No. 09/682,526
Page 21 of 30

The teachings of Bailey and Cane have been discussed above. Walmsley teaches "a consumable authentication method for validating the existence of an untrusted chip. A random number is encrypted using a first key and sent to an untrusted chip. In the untrusted chip it is decrypted using a secret key and re-encrypted together with a data message read from the untrusted chip. This is decrypted so that a comparison can be with the generated random number and the read data message." (See Walmsley, Abstract.)

As discussed above with respect to Appellant's independent claim 1, the combination of Bailey and Cane fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Cane fail to disclose the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. (See Appellant's claim 1, *supra*). Furthermore, Walmsley fails to bridge the substantial gap left by Bailey and Cane. Walmsley only teaches a consumable authentication method for validating the existence of an untrusted chip. (See Walmsley, Abstract.)

Since Bailey in view of Cane, and in further view of Walmsley do not make obvious the Appellant's invention as recited in Appellant's independent claim 1, dependent claim 3 is also not made obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 3 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellant contends that the combination of Bailey, Cane, and Walmsley does not teach the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with the authentication code being an HMAC, as set forth in claim 3. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged combination of

BRIEF ON APPEAL
Serial No. 09/682,526
Page 22 of 30

Bailey, Cane with Walmsley. Thus, the Appellant respectfully submits that claim 3 is patentable under the provisions of 35 U.S.C. §103.

2. Claim 7

The Examiner has rejected claim 7 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Cane, and in further view of Walmsley. Appellants respectfully traverse the rejection.

The teachings of Bailey, Cane and Walmsley have been discussed above.

As discussed above with respect to Appellant's independent claim 5, the combination of Bailey and Cane fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Cane fail to disclose the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle. (See Appellant's claim 5, *supra*). Furthermore, Walmsley fails to bridge the substantial gap left by Bailey and Cane. Walmsley only teaches a consumable authentication method for validating the existence of an untrusted chip. (See Walmsley, Abstract.)

Since Bailey in view of Cane, and in further view of Walmsley do not make obvious the Appellant's invention as recited in Appellant's independent claim 5, dependent claim 7 is also not made obvious since the claim depends directly from claim 5 and recites additional features of the present invention. Thus, claim 7 should be deemed patentable for at least the reasons stated above with respect to independent claim 5.

Secondly, the Appellant contends that the combination of Bailey, Cane, and Walmsley does not teach the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with the authentication code being an HMAC, as set forth in claim 7. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged

BRIEF ON APPEAL
Serial No. 09/682,526
Page 23 of 30

combination of Bailey, Cane with Walmsley. Thus, the Appellant respectfully submits that claim 7 is patentable under the provisions of 35 U.S.C. §103.

3. Claim 11

The Examiner has rejected claim 11 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Cane, and in further view of Walmsley. Appellants respectfully traverse the rejection.

The teachings of Bailey, Cane and Walmsley have been discussed above.

As discussed above with respect to Appellant's independent claim 9, the combination of Bailey and Cane fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Cane fail to disclose the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. (See Appellant's claim 9, *supra*). Furthermore, Walmsley fails to bridge the substantial gap left by Bailey and Cane. Walmsley only teaches a consumable authentication method for validating the existence of an untrusted chip. (See Walmsley, Abstract.)

Since Bailey in view of Cane, and in further view of Walmsley do not make obvious the Appellant's invention as recited in Appellant's independent claim 9, dependent claim 11 is also not made obvious since the claim depends directly from claim 9 and recites additional features of the present invention. Thus, claim 11 should be deemed patentable for at least the reasons stated above with respect to independent claim 9.

Secondly, the Appellant contends that the combination of Bailey, Cane, and Walmsley does not teach the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle

BRIEF ON APPEAL
Serial No. 09/682,526
Page 24 of 30

in combination with the authentication code being an HMAC, as set forth in claim 11. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged combination of Bailey, Cane with Walmsley. Thus, the Appellant respectfully submits that claim 11 is patentable under the provisions of 35 U.S.C. §103.

4. Claim 15

The Examiner has rejected claim 15 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Cane, and in further view of Walmsley. Appellants respectfully traverse the rejection.

The teachings of Bailey, Cane and Walmsley have been discussed above.

As discussed above with respect to Appellant's independent claim 13, the combination of Bailey and Cane fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Cane fail to disclose the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle. (See Appellant's claim 13, *supra*). Furthermore, Walmsley fails to bridge the substantial gap left by Bailey and Cane. Walmsley only teaches a consumable authentication method for validating the existence of an untrusted chip. (See Walmsley, Abstract.)

Since Bailey in view of Cane, and in further view of Walmsley do not make obvious the Appellant's invention as recited in Appellant's independent claim 13, dependent claim 15 is also not made obvious since the claim depends directly from claim 13 and recites additional features of the present invention. Thus, claim 15 should be deemed patentable for at least the reasons stated above with respect to independent claim 13.

Secondly, the Appellant contends that the combination of Bailey, Cane, and Walmsley does not teach the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key

BRIEF ON APPEAL
Serial No. 09/682,526
Page 25 of 30

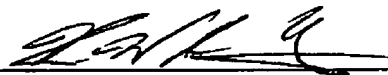
from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with the authentication code being an HMAC, as set forth in claim 15. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged combination of Bailey, Cane with Walmsley. Thus, the Appellant respectfully submits that claim 15 is patentable under the provisions of 35 U.S.C. §103.

CONCLUSION

For the reasons advanced above, the Appellant respectfully urges that the rejections of claims 1-16 as being unpatentable under 35 U.S.C. §103 are improper. Reversal of the rejections in this appeal is respectfully requested. If necessary, please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 20-0782/ATT2000-0415, and please credit any excess fees to the above referenced deposit account.

Respectfully submitted,

April 17, 2006


Kin-Wah Tong
Attorney Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Suite 100
Shrewsbury, NJ 07702

BRIEF ON APPEAL
Serial No. 09/682,526
Page 26 of 30

CLAIMS APPENDIX

1. A method of backing up one or more files on a local device onto remote servers over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

compressing one or more files and adding each of the files to a bundle;

generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and

encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.

2. The invention of claim 1 wherein the bundle is encrypted using a strong block cipher.

3. The invention of claim 1 wherein the authentication code is an HMAC.

4. The invention of claim 1 wherein the cryptographic keys contain at least 128 bits.

5. A method of restoring one or more files on remote servers to a local device over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

decrypting a bundle received from the remote server using the second cryptographic key;

checking an authentication code in the bundle using the first cryptographic key; and

decompressing one or more files from the bundle.

6. The invention of claim 5 wherein the bundle was encrypted using a strong block cipher.

7. The invention of claim 5 wherein the authentication code is an HMAC.

BRIEF ON APPEAL
Serial No. 09/682,526
Page 27 of 30

8. The invention of claim 5 wherein the cryptographic keys contain at least 128 bits.
9. A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:
- deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
 - compressing one or more files and adding each of the files to a bundle;
 - generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
 - encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.
10. The invention of claim 9 wherein the bundle is encrypted using a strong block cipher.
11. The invention of claim 9 wherein the authentication code is an HMAC.
12. The invention of claim 9 wherein the cryptographic keys contain at least 128 bits.
13. A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:
- deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
 - decrypting a bundle received from the remote server using the second cryptographic key;
 - checking an authentication code in the bundle using the first cryptographic key; and
 - decompressing one or more files from the bundle.
14. The invention of claim 13 wherein the bundle was encrypted using a strong block cipher.

BRIEF ON APPEAL
Serial No. 09/682,526
Page 28 of 30

15. The invention of claim 13 wherein the authentication code is an HMAC.
16. The invention of claim 13 wherein the cryptographic keys contain at least 128 bits.

BRIEF ON APPEAL
Serial No. 09/682,526
Page 29 of 30

EVIDENCE APPENDIX

None

BRIEF ON APPEAL
Serial No. 09/682,526
Page 30 of 30

RELATED PROCEEDINGS APPENDIX

None